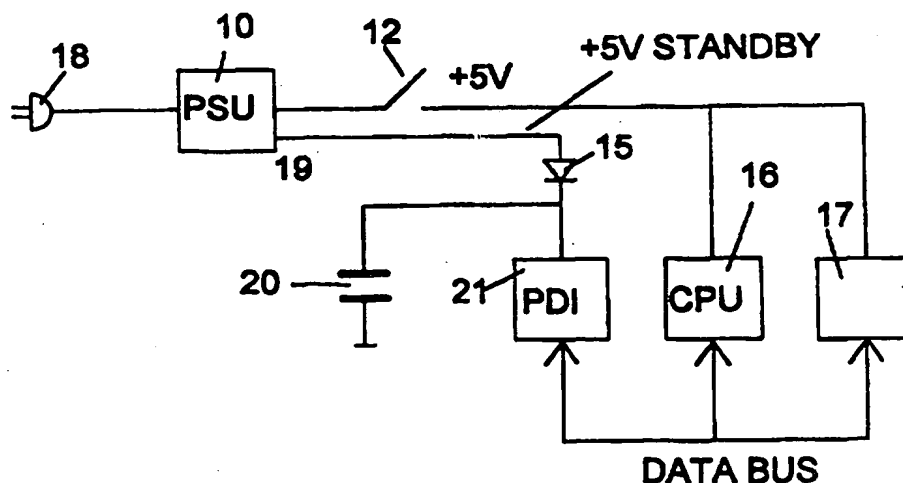




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G08B 13/14, G06F 1/30, 1/00	A1	(11) International Publication Number: WO 96/18175 (43) International Publication Date: 13 June 1996 (13.06.96)
(21) International Application Number: PCT/EP95/04806 (22) International Filing Date: 1 December 1995 (01.12.95) (30) Priority Data: 9424474.6 3 December 1994 (03.12.94) GB (71) Applicant (for all designated States except US): ICL SYSTEMS AB [SE/SE]; P.O. Box 40, S-164 93 Kista (SE). (72) Inventor; and (75) Inventor/Applicant (for US only): SJOOQUIST, Peter, Bertil, Tom [SE/SE]; Sandbacksgatan 15B, S-582 25 Linköping (SE). (74) Agent: DUPUY, Susan, Mary; Intellectual Property Dept., International Computers Limited, Cavendish Road, Stevenage, Herts SG1 2DY (GB).		(81) Designated States: US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>

(54) Title: THEFT PROTECTION FOR ELECTRICALLY-POWERED ARTICLES



(57) Abstract

A system and method for protecting an electrically-powered article, particularly a computer system such as a personal computer, from theft by rendering it effectively useless to anybody but the rightful user/owner. The personal computer includes a power disruption indicator (21) to which electrical power must be applied even when the computer is shut-down (switched off at switch 12). The continuous power is normally provided by means of a mains-supplied power unit (10). In the event of mains supply discontinuities longer than a predetermined short time period, as would be the case if the equipment is stolen, subsequent start-up of the computer is prevented until a theft protection password is provided by a potential user. A separate power source, such as a capacitor (20), is provided to power the power disruption indicator for shorter time periods, such as when moving the computer within premises, and thus obviate the need to enter the theft protection password upon such occasions.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

-1-

THEFT PROTECTION FOR ELECTRICALLY-POWERED ARTICLES

This invention relates to providing theft protection for electrically-powered articles, particularly computer systems such as personal computers, mainly from homes and small businesses, by making the article (personal computer) unusable by the thief.

In Figure 1 of the accompanying drawings there is schematically shown a conventional personal computer. It includes a power supply unit (PSU) 10 which is connected by a plug 18 to a mains supply (not shown) and which supplies the whole computer with power when the mains switch 12 is closed ie the computer is switched on. A real time clock (RTC) 11 is powered from the PSU 10 when the computer is switched on by switch 12 or from a battery 13 when the computer is switched off at switch 12. Diodes 14 and 15 schematically show how the battery 13 is connected so that it only powers RTC 11 while the computer is switched off. The RTC 11 includes a flip-flop (not shown) which is set by the RTC when the RTC detects loss of power, for instance when the battery is flat. The central processing unit (CPU) 16 can read the output of the flip-flop and can thus update the RTC with the correct time when that is input by a user after power to the RTC has been lost. The CPU resets the flip-flop after the RTC has been updated. The system also includes a program store 17.

The use of passwords to prevent unauthorised use of computer systems is commonplace. However, password protection does not prevent theft, that is provide theft protection, as the password(s) can be disabled by either removing power to the RTC, ie removing or shorting the battery, or by shorting a jumper specially designed for

CONFIRMATION COPY

-2-

this purpose. This type of password protection, furthermore, requests that the password be entered every time the system is started, which is unsuitable for theft protection.

Theft protection schemes which use a unique serial number that must be input every time the system is powered are common, for example, with car stereos, which must have the serial number input after every disconnection or replacement of the car's battery. The serial number is fixed and cannot be changed by the user. The serial number does not, however, provide protection against unauthorised use of the system once it is powered.

An object of the invention is to provide theft protection to computer systems, such as personal computer systems by making the system useless to anybody but the rightful owner. Preferably this should be achieved in such a manner that it does not impair the productivity of the rightful owner (user) by requesting user action, such as the inputting of passwords, when they are not needed.

According to one aspect of the present invention there is provided a method for protecting an electrically-powered article from theft, the article including an electrical element to which electrical power is required to be supplied even when the article is not in operation, the method including the steps of normally providing said power by means of a power supply external to the article; in the event of disconnection from the power supply, providing said power for up to a predetermined short time period from an alternative source within the article; providing means whereby the existence of a power discontinuity immediately following

-3-

the expiry of the predetermined time period can be subsequently detected, and preventing operation of the article upon detection of a said power discontinuity until a correct theft protection password has been provided by a potential operator.

According to another aspect of the present invention there is provided a method of protecting a computer system from theft, the system including an element to which electrical power is required to be supplied even when the system is shut down, the method including the steps of: normally providing said power by a mains-supplied power unit; in the event of discontinuities in the mains supply providing said power for up to a predetermined short time interval from an alternative source within the system; detecting the occurrence of mains supply discontinuities longer than the predetermined time interval, and preventing start-up of the system subsequent to such an occurrence until a correct theft prevention password has been provided by a potential user.

According to a further aspect of the present invention there is provided a computer system provided with theft protection, the system including a mains-supplied power unit; an element to which electrical power is required to be supplied even when the system is shut down, the element being connected to said power unit and normally being powered thereby; means for supplying said power for a short predetermined time interval, in the event of mains supply discontinuities, being connected to the element; and including means for detecting the occurrence of mains supply discontinuities longer than the predetermined time interval and preventing start-up of the system subsequent to such an occurrence until a correct theft protection password has been provided by a

-4-

potential user.

Embodiments of the invention will now be described with reference to the accompanying drawings, in which

Figure 1 illustrates, schematically, a conventional personal computer system, and

Figure 2 illustrates, schematically, an embodiment of a personal computer system with theft protection implemented.

The system illustrated in Figure 2 employs various components identical to those in the conventional arrangement of Figure 1 and hence employs the same reference numerals. In particular it includes a plug 18, a PSU 10, a main switch 12, a CPU 16 and a program store 17. Instead of RTC 11 there is illustrated a power disruption indicator 21 (PDI). This may be comprised by any simple or complex device which can detect a disruption in power and set a flip-flop (that can be reset by the host CPU 16) eg a simple state machine. The PDI includes the flip-flop (not shown). Typically the PDI can be the same circuit as already is used for indicating the state of the computer's 5V front contact breaker, for handling the computer's operation of 110 and 220 V etc, and for handling the PC when signals are coming from a serial port through a modem eg an incoming fax. The PDI could alternatively be an RTC. Diode 15 of Figure 2 may, however, have a different rating to that of Figure 1. The PSU 10 of Figure 2 provides a +5V stand-by power supply at port 19 which is independent of the main switch 12. The +5V stand-by power is available whenever the system is connected to the mains supply by plug 18. The battery 13 of the conventional Figure 1 arrangement is replaced by a

capacitor 20 in the embodiment of Figure 2. The capacitor 20 powers the PDI 21 for relatively short mains failures and for the time it takes to move the system within the premises, and is rated accordingly. Whenever the system is disconnected from the mains supply for a longer time, which could be the result of a theft, the CPU 18 is able to detect this by using the power lost flip-flop within the PDI. Another difference over the conventional system of Figure 1 is that in the system of Figure 2, the program store, which is non-volatile, contains a password for theft prevention.

When the system is reconnected to the mains after a short mains interruption and switched on by the user via mains switch 12, the CPU 16 will detect that the PDI has not lost power, due to the capacitor 20, and will thus not request the user to input the theft protection password.

If, however, the system has been disconnected from the mains supply for a longer time and then reconnected and switched on, the CPU 16 will detect, by reading the power lost flip-flop in the PDI, that the system has been disconnected and will therefore request that the user inputs the theft prevention password, effectively rendering the system useless for everybody except the legitimate owner. The owner of the system has the possibility, using a set-up program, to change the theft prevention password or to disable theft prevention completely.

A typical post start-up sequence to implement theft protection could be as follows:

-6-

```
PowerOn:
InitializeKeyboardAndDisplay ();
if(PDIHasLostPower) {
    if (TheftProtectionEnabled) {
        /* Do not return until a correct
        password has been entered
*/
        RequestAndCheckAdminPassword ();
    }
    /* Clear PowerLost status of PDI*/
    Initialize PDI ();
}
/* Normal start-up sequence follows here */
```

As will be appreciated from the above, the invention uses a novel method of powering the PDI together with a password stored in a non-volatile memory 17 and a special start-up program to achieve theft prevention/protection. The same password can also be used to prevent unauthorised use of the system, if desired. If there has been no detectable power loss, the theft protection password is not required to be entered at start-up. Theft prevention is thus provided for a computer system by using standard components together with other readily available components and appropriate software. Whilst powering of the PDI is referred to above, the invention could equally be applied to powering of any other element which requires a continuous supply, even when the computer is shutdown/switched off. Furthermore the basic principle of detecting when a powered unit is disconnected from a power source for more than a short time period and in that case requiring the input of a "password" before it can be made to work again, can be applied to other electrically powered articles than personal computers for example TV receivers and VCRs. The theft prevention

-7-

password may in this case comprise a code number rather than involving letters as implied by a password. The latter may of course involve, letter, numerals and other elements.

In general terms, the invention thus protects an electronically-powered article (computer system) from theft, the article including an element which requires power at all times, but only very little current. This power is normally supplied by a mains or battery supply unit external to the article. If that supply unit is disconnected for longer than a short predetermined time period, the power is supplied from an alternative source within the article for up to the short predetermined time period. After that time, if the supply unit has not already been reconnected, it will not be possible to use the article unless a correct theft protection password is inserted by a potential user, due to "tripping" of an element within the article which can only be reset as a result of a correct password being entered.

CLAIMS

1. A method for protecting an electrically-powered article from theft, the article including an electrical element to which electrical power is required to be supplied even when the article is not in operation, the method including the steps of normally providing said power by means of a power supply external to the article; in the event of disconnection from the power supply, providing said power for up to a predetermined short time period from an alternative source within the article; providing means whereby the existence of a power discontinuity immediately following the expiry of the predetermined time period can be subsequently detected, and preventing operation of the article upon detection of a said power discontinuity until a correct theft protection password has been provided by a potential operator.
2. A method of protecting a computer system from theft, the system including an element to which electrical power is required to be supplied even when the system is shut down, the method including the steps of: normally providing said power by a mains-supplied power unit; in the event of discontinuities in the mains supply providing said power for up to a predetermined short time interval from an alternative source within the system; detecting the occurrence of mains supply discontinuities longer than the predetermined time interval, and preventing start-up of the system subsequent to such an occurrence until a correct theft prevention password has been provided by a potential user.

3. A method as claimed in Claim 2, wherein the system includes a processing unit and a memory unit and the element is a power disruption indicator including a flip-flop which is set at the expiry of the predetermined time interval, and wherein the detecting step comprises causing the processing unit to read the state of the flip-flop, and wherein, in the event of the flip-flop being set, upon start-up of the system the processing unit requests the insertion of the theft prevention password and only permits start-up if it corresponds to a password stored in the memory unit.
4. A method as claimed in Claim 2 or Claim 3, wherein the system includes a main switch and the power unit is coupled to the processing unit and the memory unit only when the main switch is closed, whereas the element is connected directly to the power unit and is connected to the alternative source in the event of mains supply discontinuities.
5. A method as claimed in any one of the Claims 2-4, wherein the alternative source is a capacitor chargeable by the power unit.
6. A computer system provided with theft protection, the system including a mains-supplied power unit; an element to which electrical power is required to be supplied even when the system is shut down, the element being connected to said power unit and normally being powered thereby; means for supplying said power for a short predetermined time interval, in the event of mains supply discontinuities, being connected to the element; and including means for

-10-

detecting the occurrence of mains supply discontinuities longer than the predetermined time interval and preventing start-up of the system subsequent to such an occurrence until a correct theft protection password has been provided by a potential user.

7. A computer system as claimed in Claim 6, wherein the element is a power disruption indicator, and wherein the detection and prevention means are comprised by a processing unit and a memory unit.
8. A computer system as claimed in Claim 7, wherein the power disruption indicator includes a flip-flop which is set in the event of a mains discontinuity longer than the predetermined time interval, and wherein the processing means reads the state of the flip-flop to determine if there have been any said occurrences.
9. A computer system as claimed in Claim 7 or Claim 8, wherein the processing unit and the memory unit are connected to the power unit via a main switch, which is open when the system is shut down but closed by the action of a user when start-up is required.
10. A computer system as claimed in any one of Claims 5-8, wherein the means for supplying the power for the predetermined time interval is a capacitor, chargeable by the power unit.

1/1

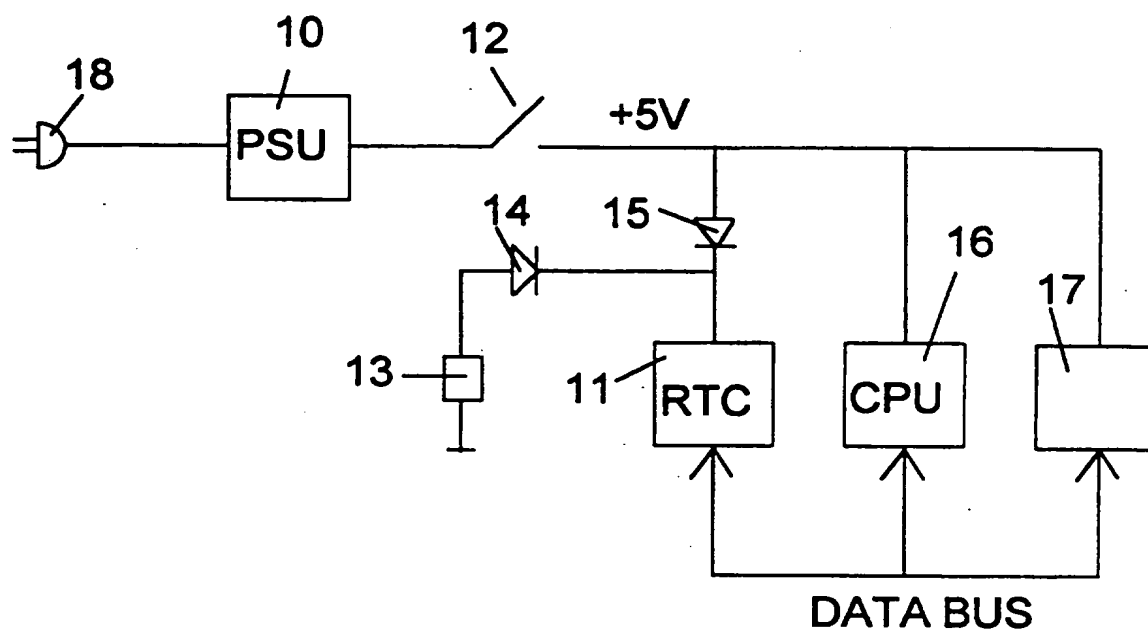


FIG 1

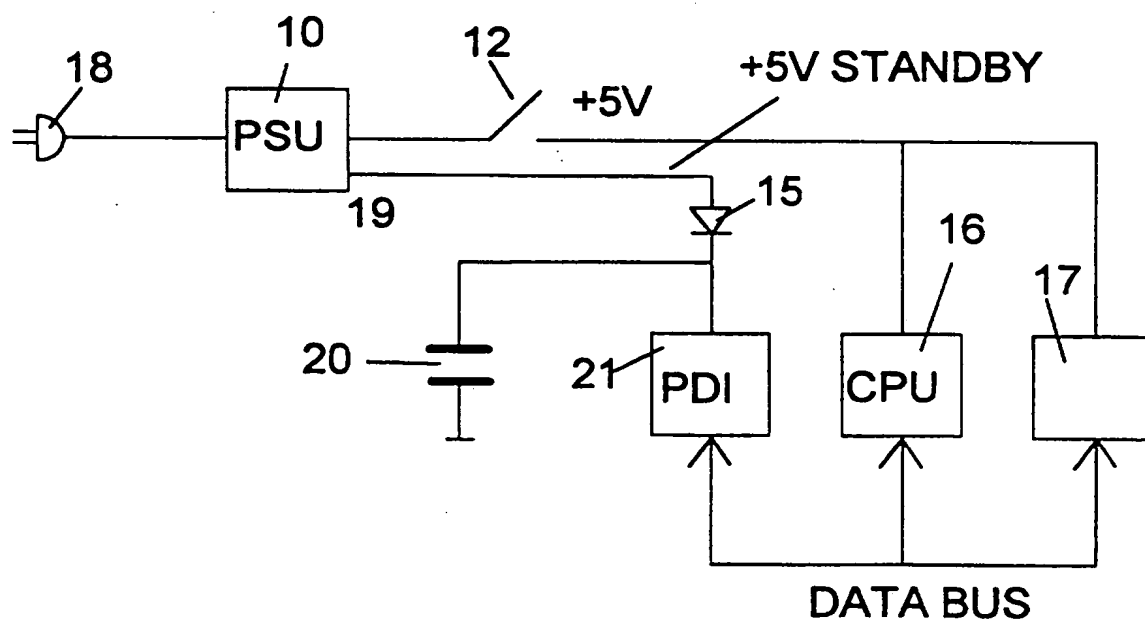


FIG 2

INTERNATIONAL SEARCH REPORT

International Application No

PL EP 95/04806

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 G08B13/14 G06F1/30 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G08B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP,A,0 145 405 (INTERNATIONAL ELECTRONIC TECHNOLOGY) 19 June 1985 see the whole document	1,2,4,7
Y		3,5,6, 8-12
Y	US,A,4 584 651 (CAREY, JR. ET AL) 22 April 1986 see the whole document	3,6, 8-10,12
Y	EP,A,0 458 510 (MARTIN) 27 November 1991 see abstract	5,6,11, 12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

1 April 1996

Date of mailing of the international search report

22. 04. 96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax (+31-70) 340-3016

Authorized officer

Powell, D

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/EP 95/04806

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-0145405	19-06-85	US-A- 4494114 CA-A- 1211542 JP-A- 60138645	15-01-85 16-09-86 23-07-85
US-A-4584651	22-04-86	NONE	
EP-A-0458510	27-11-91	US-A- 5111058 AU-B- 637556 AU-B- 7595791 CA-A,C 2041179 JP-A- 4229034	05-05-92 27-05-93 28-11-91 24-11-91 18-08-92